Proc. Indian Acad. Sci. (Math. Sci.) Vol. 116, No. 1, February 2003, pp. 1–8.
Printed in India

Arithmetic properties of the Ramanujan function

FLORIAN LUCA[1] and IGOR E SHPARLINSKI[2]

[1]Instituto de Matemáticas, Universidad Nacional Autónoma de México, C.P. 58089, Morelia, Michoacán, México
[2]Department of Computing, Macquarie University, Sydney, NSW 2109, Australia
E-mail: fluca@matmor.unam.mx; igor@ics.mq.edu.au

MS received 2 December 2004

Dedicated to T N Shorey on his sixtieth birthday

Abstract. We study some arithmetic properties of the Ramanujan function $\tau(n)$, such as the largest prime divisor $P(\tau(n))$ and the number of distinct prime divisors $\omega(\tau(n))$ of $\tau(n)$ for various sequences of n. In particular, we show that $P(\tau(n)) \geq (\log n)^{33/31+o(1)}$ for infinitely many n, and

$$P(\tau(p)\tau(p^2)\tau(p^3)) > (1+o(1))\frac{\log\log p \log\log\log p}{\log\log\log\log p}$$

for every prime p with $\tau(p) \neq 0$.

Keywords. Ramanujan τ-function; applications of $\mathscr{S}$-unit equations.

1. Introduction

Let $\tau(n)$ denote the *Ramanujan function* defined by the expansion

$$X\prod_{n=1}^{\infty}(1-X^n)^{24} = \sum_{n=1}^{\infty}\tau(n)X^n, \qquad |X|<1.$$

For any integer n we write $\omega(n)$ for the number of distinct prime factors of n, $P(n)$ for the largest prime factor of n and $Q(n)$ for the largest square-free factor of n with the convention that $\omega(0)=\omega(\pm 1)=0$ and $P(0)=P(\pm 1)=Q(0)=Q(\pm 1)=1$.

In this note, we study the numbers $\omega(\tau(n))$, $P(\tau(n))$ and $Q(\tau(n))$ as n ranges over various sets of positive integers.

The following basic properties of $\tau(n)$ underline our approach which is similar to those of [9,13]:

- $\tau(n)$ is an integer-valued multiplicative function; that is, $\tau(m)\tau(n)=\tau(mn)$ if $\gcd(m,n)=1$.
- For any prime p, and an integer $r\geq 0$, $\tau(p^{r+2}) = \tau(p^{r+1})\tau(p) - p^{11}\tau(p^r)$, where $\tau(1)=1$.

In particular, the identity

$$\tau(p^2) = \tau(p)^2 - p^{11} \tag{1}$$

plays a crucial role in our arguments.

It is also useful to recall that by the famous result of Deligne

$$|\tau(p)| \le 2p^{11/2} \quad \text{and} \quad |\tau(n)| \le n^{11/2+o(1)} \tag{2}$$

for any prime p and positive integer n (see [7]).

One of the possible approaches to studying arithmetic properties of $\tau(n)$ is to remark that the values $u_r = \tau(2^r)$ form a Lucas sequence satisfying the following binary recurrence relation

$$u_{r+2} = -24u_{r+1} - 2048u_r, \qquad r = 0, 1, \ldots, \tag{3}$$

with the initial values $u_0 = 1$, $u_1 = -24$. By the primitive divisor theorem for Lucas sequences which claims that each sufficiently large term u_r has at least one new prime divisor (see [2] for the most general form of this assertion), we conclude that

$$\omega\left(\prod_{r\le z} \tau(2^r)\right) \ge z + O(1),$$

leading to the inequality

$$\omega\left(\prod_{\substack{n\le x\\ \tau(n)\ne 0}} \tau(n)\right) \ge \left(\frac{1}{\log 2} + o(1)\right)\log x$$

as $x \to \infty$. In particular, we derive that for infinitely many n,

$$P(\tau(n)) \ge \log n \log\log n.$$

A stronger conditional result, under the *ABC*-conjecture, is given in [10]. We also have

$$Q(\tau(n)) \ge n^{(\log 2+o(1))/\log\log\log n}$$

for infinitely many n (see eq. (16) in [14]).

Furthermore, since $u_r | u_s$, whenever $r+1 | s+1$, it follows that if for sufficiently large s we set $k = \mathrm{lcm}[2, \ldots, s+1] - 1$, then $\tau(2^k)$ is divisible by $\tau(2^r)$ for all $r \le s$. Thus, setting $n = 2^k$ we get

$$\omega(\tau(n)) \ge s + O(1) = \left(\frac{1}{\log 2} + o(1)\right)\log k \ge \left(\frac{1}{\log 2} + o(1)\right)\log\log n$$

as $n \to \infty$. Here, we use different approaches to improve on these bounds.

Our results are based on some bounds for smooth numbers, that is, integers n with restricted $P(n)$ (see [5,16]). We also use results on $\mathscr{S}$-unit equations (see [3]). We recall that for a given finite set of primes $\mathscr{S}$, a rational $u = s/t \ne 0$ with $\gcd(s,t) = 1$ is called an $\mathscr{S}$-unit if all prime divisors of both s and t are contained in $\mathscr{S}$. Finally, we also use bounds on linear forms in q-adic logarithms (see [17]).

We recall that in [8] it is shown under the extended Riemann hypothesis that $\omega(\tau(p)) \sim \log\log p$ holds for almost all primes p and that $\omega(\tau(N)) \sim 0.5(\log\log N)^2$ holds for almost all positive integers N.

Throughout the paper, the implied constants in the symbols 'O', '$\gg$' and '$\ll$' are absolute (recall that the notations $U \ll V$ and $V \gg U$ are equivalent to the statement that $U = O(V)$ for positive functions U and V). We also use the symbol 'o' with its usual meaning: the statement $U = o(V)$ is equivalent to $U/V \to 0$.

We always use the letters p and q to denote prime numbers.

2. Divisors of the Ramanujan function

Theorem 1. *There exist infinitely many n such that $\tau(n) \neq 0$ and $P(\tau(n)) \geq (\log n)^{33/31+o(1)}$.*

Proof. For a constant $A > 0$ and a real z we define the set

$$\mathscr{S}_A(z) = \{n \leq z \colon P(n) \leq (\log n)^A\}.$$

For every $A > 1$, we have $\#\mathscr{S}_A(z) = z^{1-1/A+o(1)}$, as $z \to \infty$ (see eq. (1.14) in [5] or Theorem 2 in § III.5.1 of [16]).

Let $x > 0$ be sufficiently large. By a result of Serre [11], the estimate $\#\{p \leq y \colon \tau(p) = 0\} \ll y/(\log y)^{3/2}$ holds as y tends to infinity. Applying this estimate with $y = x^{1/2}$, it follows that there are only $o(\pi(y))$ primes $p < y$ such that $\tau(p) = 0$. It is also obvious from (1) that $\tau(p^2) \neq 0$.

Assume that for some A with $1 < A < 33/31$, we have the inequality $P(\tau(p)\tau(p^2)) \leq (\log y)^A$ for all remaining primes $p \leq y$. We see from (1) and (2) that $|\tau(p^2)| = |\tau(p)^2 - p^{11}| \leq 3p^{11} \leq 3y^{11}$. Denoting $z_1 = 3y^{11}$ and $z_2 = 2p^{11/2}$, we deduce that for $(1+o(1))\pi(y) = y^{1+o(1)}$ primes $p < y$ with $\tau(p) \neq 0$, we have a representation $p^{11} = s_1^2 - s_2$, where $s_i \in \mathscr{S}_A(z_i)$, $i = 1, 2$. Thus

$$y^{1+o(1)} \leq \#\mathscr{S}_A(z_1)\#\mathscr{S}_A(z_2) \leq (z_1 z_2)^{1-1/A+o(1)} \leq (6y^{33/2})^{1-1/A+o(1)},$$

which is impossible for $A < 33/31$. This completes the proof. $\square$

We remark in passing that the above proof shows that the inequality $P(\tau(p)\tau(p^2)) > (\log p)^{33/31+o(1)}$ holds for almost all primes p.

Theorem 2. *The estimate*

$$\omega\left(\prod_{\substack{p<x^{1/3}\\ \tau(p)\neq 0}} \tau(p)\tau(p^2)\tau(p^3)\right) \geq \left(\frac{1}{6\log 7} + o(1)\right)\log x$$

holds as x tends to infinity.

Proof. Let x be a large positive integer and put $y = x^{1/3}$. Let $\mathscr{R}$ be the set of odd primes $p \leq y$ such that $\tau(p) \neq 0$. Note that since $\tau(p) \neq 0$, it follows that $\tau(p^2) \neq 0$ and $\tau(p^3) \neq 0$. Let

$$M = \prod_{p \in \mathscr{R}} \tau(p)\tau(p^2)\tau(p^3) \quad \text{and} \quad s = \omega(M).$$

Since $\tau(p^2)=\tau(p)^2-p^{11}$ and $\tau(p^3)=\tau(p)(\tau(p)^2-2p^{11})$, eliminating p^{11}, we get the equation

$$1=\frac{2\tau(p^2)}{\tau(p)^2}-\frac{\tau(p^3)}{\tau(p)^3}.$$

We claim that the rational numbers $2\tau(p^2)/\tau(p)^2$ are distinct for distinct odd primes. Indeed, if $\tau(p_1^2)/\tau(p_1)^2=\tau(p_2^2)/\tau(p_2)^2$ for two distinct odd primes p_1,p_2, we get that $p_1^{11}/\tau(p_1)^2=p_2^{11}/\tau(p_2)^2$, or $p_1^{11}\tau(p_2)^2=p_2^{11}\tau(p_1)^2$. Therefore, $p_1^{11}|\tau(p_1)^2$. Thus, $p_1^{12}|\tau(p_1)^2$, which is impossible for $p_1>3$ because of (2), and can be checked by hand to be impossible for $p_1=3$.

Let $\mathscr{S}$ be the set of all prime divisors of M. Thus, $\#\mathscr{S}=s$. We see that the equation $u-v=1$ has $\#\mathscr{R}$ distinct solutions in the $\mathscr{S}$-units

$$(u,v)=\left(\frac{2\tau(p^2)}{\tau(p)^2},\frac{\tau(p^3)}{\tau(p)^3}\right). \tag{4}$$

It is known (see [3]), that the number of solutions of such a $\mathscr{S}$-unit equation is $O(7^{2s})$. We thus get that $7^{2s}\gg\#\mathscr{R}=(1+o(1))\pi(y)$, giving

$$s\geq\frac{1}{6\log 7}(1+o(1))\log x$$

as $x\to\infty$, which finishes the proof. □

Theorem 3. *The estimate*

$$P(\tau(p)\tau(p^2)\tau(p^3))>(1+o(1))\frac{\log\log p\log\log\log p}{\log\log\log\log p}$$

holds as p tends to infinity through primes such that $\tau(p)\neq 0$.

Proof. As in the proof of Theorem 2, we consider the equation $u-v=1$, having the solution (4) for every prime p with $\tau(p)\neq 0$. Write

$$u=E/D \quad \text{and} \quad v=F/D,$$

where D is the smallest positive common denominator of u and v. Then

$$E=Du=2D-2p^{11}D/\tau(p)^2 \quad \text{and} \quad F=Dv=D-2Dp^{11}/\tau(p)^2$$

are integers with $\gcd(E,F)=1$, and since $E-F=D$, we also have $\gcd(D,E)=\gcd(D,F)=1$.

We note the inequalities

$$D\ll p^{11} \quad \text{and} \quad p\ll\max\{|E|,|F|\}\ll p^{22}. \tag{5}$$

Indeed, the upper bounds follow directly from (2). It also follows from (2) that $p^6\nmid\tau(p)$. This shows that $p^{11}/\tau(p)^2$ is a rational number whose numerator is a multiple of p. In particular,

$$E-2F=\frac{2Dp^{11}}{\tau(p)^2}\geq p,$$

which implies the lower bound in (5).

We have $P(\tau(p)\tau(p^2)\tau(p^3)) \ge \ell$, where $\ell = P(EDF)$.

Let $t = \omega(\tau(p)\tau(p^2)\tau(p^3))$. By (5), we see that there exists a prime q and a positive integer α such that q^α divides one of E or F and $q^\alpha \gg p^{1/t}$.

First we assume that $q^\alpha | E = D - F$, and write

$$D = \prod_{j=1}^{t} q_j^{\beta_j} \quad \text{and} \quad F = \prod_{j=1}^{t} q_j^{\gamma_j},$$

with some primes q_j and non-negative integers β_j, γ_j such that $\min\{\beta_j, \gamma_j\} = 0$ for all $j = 1, \ldots, t$ (clearly, $\beta_i = \gamma_i = 0$ for $q_i = q$). By (5), we also have

$$B = \max_{j=1,\ldots,t} \{\beta_j, \gamma_j\} \ll \max\{\log D, \log |E|\} \ll \log p.$$

Using the lower bound for linear forms in q-adic logarithms of Yu [17], we derive

$$\alpha \le qc^t \log B \prod_{j=1}^{t} \log q_j \ll \ell (c \log \ell)^t \log\log p \tag{6}$$

with some absolute constant $c > 0$. Since also

$$\alpha \gg \frac{\log p}{t \log q} \ge \frac{\log p}{t \log \ell},$$

we get

$$\frac{\log p}{\log\log p} \ll \ell t (c \log \ell)^t \ll \ell (2c \log \ell)^t.$$

Hence,

$$\log\log p \le t(1 + o(1)) \log\log \ell. \tag{7}$$

By the prime number theorem (see [4]), we have

$$t \le (1 + o(1)) \frac{\ell}{\log \ell},$$

which together with (7) leads us to

$$(1 + o(1)) \frac{\log\log p \log\log\log p}{\log\log\log\log p} \le t.$$

The case $q^\alpha | F = D - E$ can be considered completely analogously which concludes the proof. □

We recall that the *ABC*-conjecture asserts that for any fixed $\varepsilon > 0$ the inequality

$$Q(abc) \gg (\max |a|, |b|, |c|)^{1-\varepsilon}$$

holds for any relatively prime integers a, b, c with $a + b = c$. Thus, in the notation of the proof of Theorem 3, we immediately conclude from (5) that the *ABC*-conjecture yields

$$Q(\tau(p)\tau(p^2)\tau(p^3)) \ge Q(DEF) \ge p^{1+o(1)}.$$

Thus, by the prime number theorem,

$$P(\tau(p)\tau(p^2)\tau(p^3)) \geq (1+o(1))\log p.$$

The best known unconditional result of Stewart and Yu [15] towards the *ABC*-conjecture implies that

$$Q(\tau(p)\tau(p^2)\tau(p^3)) \geq Q(DEF) \geq (\log p)^{3+o(1)}.$$

3. Factorials and the Ramanujan function

In [6], all the positive integer solutions (m,n) of the equation $f(m!) = n!$ were found, where f is any one of the multiplicative arithmetical functions φ, σ, d, which are the Euler function, the sum of divisors function, and the number of divisors function, respectively. Further results on such problems have been obtained by Baczkowski [1]. Here, we study this problem for the Ramanujan function.

Theorem 4. *There are only finitely many effectively computable pairs of positive integers (m,n) such that $|\tau(m!)| = n!$.*

Proof. Assume that (m,n) are positive integers such that $\tau(m!) = n!$. By (2) and the Stirling formula

$$\begin{aligned}\exp((1+o(1))n\log n) = n! = \tau(m!) < (m!)^{11/2+o(1)}\\ < \exp((11/2+o(1))m\log m),\end{aligned}$$

as m tends to infinity. Thus, we conclude that if m is sufficiently large, then $n < 6m$.

Let $\nu(m)$ be the order at which the prime 2 appears in the prime factorization of $m!$. It is clear that $\nu(m) > m/2$ if m is sufficiently large. Since τ is multiplicative, it follows that $u_{\nu(m)} = \tau(2^{\nu(m)})|n!$, where the Lucas sequence u_r is given by (3) with $u_0 = 1$, $u_1 = -24$.

For $r \geq 1$, we put $\zeta_r = \exp(2\pi i/r)$ and consider the sequence $v_r = \Phi_r(\alpha,\beta)$ where

$$\Phi_r(X,Y) = \prod_{\substack{1\leq k\leq r\\ \gcd(k,r)=1}} (X - \zeta_r^k Y).$$

It is known that $v_r|u_r$. It is also known (see [2]), that $v_r = A_r B_r$, where A_r and $B_r > 0$ are integers, $|A_r| \leq 6(r+1)$ and every prime factor of B_r is congruent to $\pm 1 \pmod{r+1}$. Let α and β be the two roots of the characteristic equation $\lambda^2 - 24\lambda - 2048 = 0$. Since both inequalities $|v_k| \leq 2|\alpha|^{k+1}$ and $|v_k| \geq |\alpha|^{k+1-\gamma\log(k+1)}$ hold for all positive integers k with some absolute constant γ (see, for example, Theorem 3.1 on p. 64 in [12]), it follows that

$$\begin{aligned}6(r+1)B_r &\geq 2^{-\tau(r+1)}\alpha^{\varphi(r+1)-\gamma\tau(r+1)\log(r+1)}\\ &= |\alpha|^{\varphi(r+1)+O(\tau(r+1)\log(r+1))}.\end{aligned}$$

Since $\varphi(r+1) \gg r/\log\log r$, and $\tau(r+1)\log(r+1) = r^{o(1)}$, the above inequality implies that

$$B_r > |\alpha|^{\varphi(r+1)/2}$$

whenever r is sufficiently large.

In particular, we see that $B_{\nu(m)}|\tau(m!)$, has all prime factors $\ell \equiv \pm 1 \,(\mathrm{mod}\ \nu(m)+1)$, and is of the size

$$B_{\nu(m)} > \exp(cm/\log\log m),$$

where c is some positive constant.

However, since $B_{\nu(m)}|n!$ and $n < 6m$, it follows that all prime factors ℓ of $B_{\nu(m)}$ satisfy $\ell < 6m$. Since $\nu(m) > m/2$, there are at most 26 primes $\ell < 6m$ with $\ell \equiv \pm 1 \ (\mathrm{mod}\ \nu(m)+1)$. Furthermore, again since $B_{\nu(m)}|n!$, $n < 6m$, and all prime factors ℓ of $B_{\nu(m)}$ satisfy $\ell \equiv \pm 1 \,(\mathrm{mod}\ \nu(m)+1)$, it follows that $\ell^{14} \nmid B_{\nu(m)}$. Hence,

$$B_{\nu(m)} < (6m)^{26\cdot 13} = m^{O(1)}.$$

Comparing this with the above lower bound on $B_{\nu(m)}$, we conclude that m is bounded.

□

Acknowledgements

During the preparation of this paper, the first author was supported in part by grants SEP-CONACYT 37259-E and 37260-E, and the second author was supported in part by ARC grant DP0211459.

References

[1] Baczkowski D, Master Thesis (Miami Univ., Ohio, 2004)

[2] Bilu Y, Hanrot G and Voutier P M, Existence of primitive divisors of Lucas and Lehmer numbers, with an appendix by M Mignotte, *J. Reine Angew. Math.* **539** (2001) 75–122

[3] Evertse J-H, On equations in *S*-units and the Thue-Mahler equation, *Invent. Math.* **75** (1984) 561–584

[4] Hardy G H and Wright E M, An introduction to the theory of numbers (Oxford Univ. Press, Oxford, 1979)

[5] Hildebrand A and Tenenbaum G, Integers without large prime factors, *J. de Théorie des Nombres de Bordeaux* **5** (1993) 411–484

[6] Luca F, Equations involving arithmetic functions of factorials, *Divulg. Math.* **8(1)** (2000) 15–23

[7] Murty M R, The Ramanujan τ function, Ramanujan revisited, *Proc. Illinois Conference on Ramanujan* (1988) 269–288

[8] Murty M R and Murty V K, Prime divisors of Fourier coefficients of modular forms, *Duke Math. J.* **51** (1985) 521–533

[9] Murty M R, Murty V K and Shorey T N, Odd values of the Ramanujan τ-function, *Bull. Soc. Math. France* **115** (1987) 391–395

[10] Murty M R and Wong S, The *ABC* conjecture and prime divisors of the Lucas and Lehmer sequences, Number Theory for the Millennium, vol. III (MA: A. K. Peters, Natick) (2002) 43–54

[11] Serre J P, Quelques applications du théorème de densité de Chebotarev, *Publ. Math., Inst. Hautes Étud. Sci.* **54** (1981) 123–201

[12] Shorey T N and Tijdeman R, Exponential diophantine equations (Cambridge: Cambridge Univ. Press) (1986)

[13] Shorey T N, Ramanujan and binary recursive sequences, *J. Indian Math. Soc.* **52** (1987) 147–157

[14] Stewart C L, On divisors of Fermat, Fibonacci, Lucas and Lehmer numbers, III, *J. London Math. Soc.* **28** (1983) 211–217

[15] Stewart C L and Yu K R, On the *abc* conjecture, II, *Duke Math. J.* **108** (2001) 169–181

[16] Tenenbaum G, Introduction to analytic and probabilistic number theory (Cambridge: Cambridge Univ. Press) (1995)

[17] Yu K, *p*-Adic logarithmic forms and group varieties, II, *Acta Arith.* **89** (1999) 337–378